March 26, 2022

OVATION
AMERICAS

# April 2022 Newsletter

## Are your devices spying on you?    (Part 1)

**More and more objects and devices in the home are now connected to the internet, making them potentially at risk of being hacked.**

## From internet-connected televisions, toys, fridges, ovens, security cameras, door locks, fitness trackers and lights, the so-called “Internet of Things” (IoT) promises to revolutionise our homes.

But it also threatens to increase our vulnerability to malicious acts. Security flaws in IoT devices are commun. Hackers can exploit those vulnerabilities to take control of devices, steal or change data, and spy on us.

In recognition of these risks, many governments has introduced new code of practice to encourage manufacturers to make IoT devices more secure. The code provides guidance on secure passwords, the need for security patches, the protection and deletion of consumers’ personal data and the reporting of vulnerabilities, among other things.

The problem is that most of the time the code is voluntary. Experiences elsewhere, such as the United Kingdom, suggest a voluntary code will be insufficient to deliver the protections consumers need.

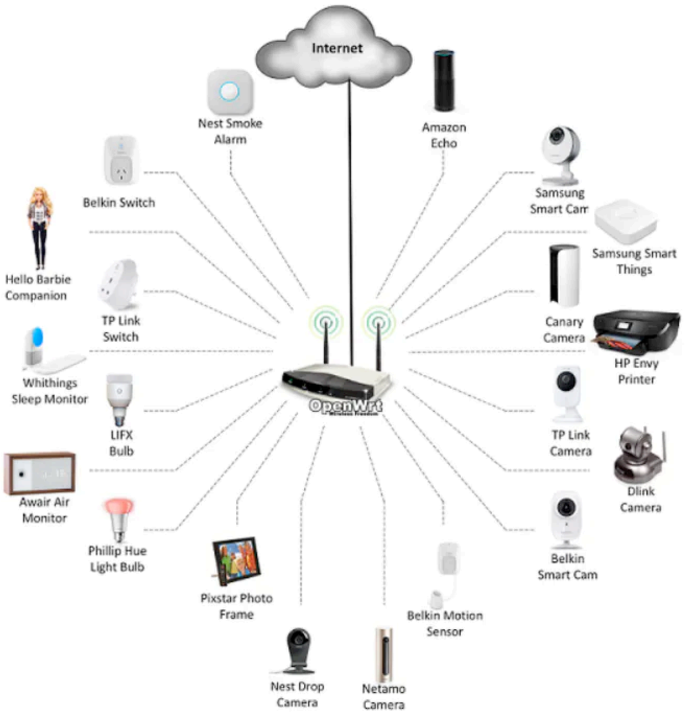
Indeed it might even increase risks, by lulling consumers into a false sense of security about the safety of the devices they buy.

# Many IoT devices are insecure

IoT devices designed for consumers are generally less secure than conventional computers.

In 2017 the Australian Communications Consumer Action Network commissioned researchers from the University of New South Wales to test the security of 20 household appliances capable of being connected and controlled via wi-fi.

These included a smart TV, portable speaker, voice assistant, printer, sleep monitor, digital photo frame, bathroom scales, light bulb, power switch, smoke alarm and Hello Barbie talking doll.



While some devices (including the Barbie) were found to be relatively secure in terms of confidentiality, all had some form of security flaw. Many “allowed potentially serious safety and security breaches”.

What this could potentially mean is that someone could, for example, hack into a household’s wi-fi network and collect data from IoT devices. It might be as simple as knowing when lights are switched on to determine when a home can be burgled. Someone with more malicious intent could turn on your oven while shutting down smoke alarms and other sensors.

## Risks to consumers, and society

Factors leading to poor security in Iot devices include manufacturers’ desires to minimise components and keep costs down. Many makers of consumer goods also have little experience with cyber-security issues.

Allied with the fact many consumers aren't technologically savvy enough to appreciate the risks and protect themselves, this creates the prospect of IoT devices being exploited.

On a personal level, you could be spied on and harassed. Personal pictures or information could be exposed to the world, or used to extort you.

On a societal level, IoT devices can be hijacked and used collectively to shut down services and networks. Even compromising one device may enable connected infrastructure to be hacked.

This is a rising concern as more people connect to workplace networks from home.

These new IoT devices often make our lives easier. IoT devices can enhance efficiency, convenience, productivity or the overall quality of our lives. But, there is always a trade off between their life enhancing value and a potential loss of privacy. Many of the convenient IoT devices we use in our home, at work, in the car or wherever we go, **also pose spying risks**. This is the case with three recently introduced IoT devices.

## Apple Air Tags

A IoT device that provides an easy way to keep track of your things. (e.g. wallet, keys, bicycle, etc.)

Features:

- Connects with your Apple device to help locate things you have tagged with the Apple AirTag
- Acts as a beacon by emanating a sound so you can locate your tagged things
- Sends a Bluetooth signal detected by nearby devices in the Find My network and sends the location of the AirTag to iCloud
- It uses Find My network (with 100 million + iPhone, iPad, and Mac devices around the world) to assist with locating your tagged things
- Use Precision Finding with an Apple iPhone 11 or later in conjunction with the Find My app and Siri to find your tagged things.

Risk:

1. A spy can connect an AirTag to their Apple device and then drop the AirTag in your pocket, handbag, backpack, car, etc. They can track your whereabouts within range of the tag in a 8-24 hour window using their iPhone. The spy can capture your location, your movements, your residence address and your frequently visited places.
2. The AirTag can be opened and reprogrammed for malicious purposes. Yes, security researchers hacked the AirTag in less than 10 days.
3. If you use an Android device, the only way to find out about the presence of an AirTag nearby is the sound emitted by the Apple AirTag. The sound starts after a period of inactivity (range 8-24 hours). But, if you can't hear the sound emitted by the AirTag and you are not using an iPhone, the spy can continue tracking you for the about a year which is about the battery life. A Tracker Detect APP for Android Now Available from Apple!

### Amazon Sidewalk

A IoT device that creates a shared "mesh" network of interconnected devices.

Features:

- Creates a low-bandwidth network using Sidewalk Bridge devices
- Shares a portion of your Internet bandwidth to a pool that provides the

services to you/your neighbors (maximum bandwidth 80Kbps, 500MB monthly per customer cap. )
- Provided by Amazon at no charge to customers
- Simplifies new device setup
- Extends the low-bandwidth working range of devices like trackers (e.g. Tile)
- Can help devices stay online even when they are out of range of your home Wi-Fi

Risk:

1. A spy/hacker connects to the Amazon Sidewalk network, uses malware to penetrate devices and conducts illegal activities with your device.
2. A neighbor's network is not properly secured, but it's connected to Amazon Sidewalk. A hacker puts ransomware on the neighbor's network/devices and the ransomeware spreads to other devices connected to the Amazon sidewalk.
3. A hacker penetrates  a network that is connected to Amazon Sidewalk and and uses it to access information on connected device(s).

**Audio Wow+**

IoT device that is a wireless mini microphone with sound effects.

Features:

- Mobile phone direct connected
- Built-in microphone
- Real-time monitoring
- 4 levels of noise reduction

- Cancel and replace original vocals
- Records phone calls and transcribes the content of the caller and receiver separately for easy editing

Risk:

1. Can be used for surreptitious recordings since its small size makes it easy to conceal.
2. Record both ends of conversation. Most devices only record the half of the conversation where the microphone is present.
3. There is a potential for voice recordings to be altered to create records/evidence of conversations that did not occur.

**What Can Be Done to Stop Cyber Eavesdropping / IoT Threat?**

Protecting your valuable information from IoT threats is essential. So, how can you prevent your security from being compromised?

Having PERIODIC TSCM / CYBER TSCM sweeps designed to detect rogue mobile devices, hidden cell phones, and other wireless eavesdropping and hacking devices and confirm that no one has compromised your own personal devices

If you want to make sure that your personal privacy is secure, feel free to contact us today! At: info@ovationamericas.com or from our website at:

www.ovationamericas.com

Security and Privacy is very much a matter of good personal habits. Let's keep learning and stay up to date on cybersecurity issues to give us the best chance of avoiding costly hacks and scams.

OVATION
AMERICAS